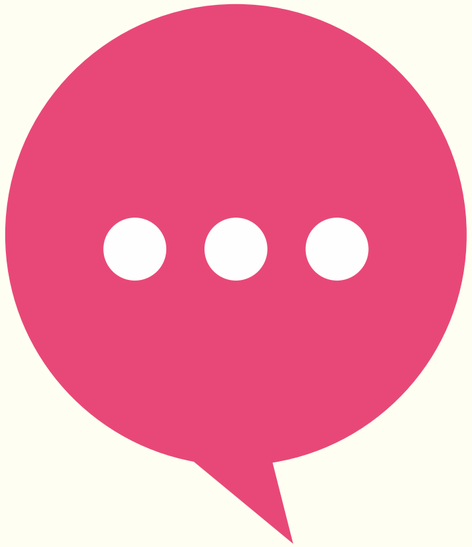
ECS
EUROPEAN CYBER SECURITY ORGANISATION



Cybersecurity Awareness Calendar

INTERNET OF THINGS

February 2021

Awareness Calendar

CYBERSECURITY

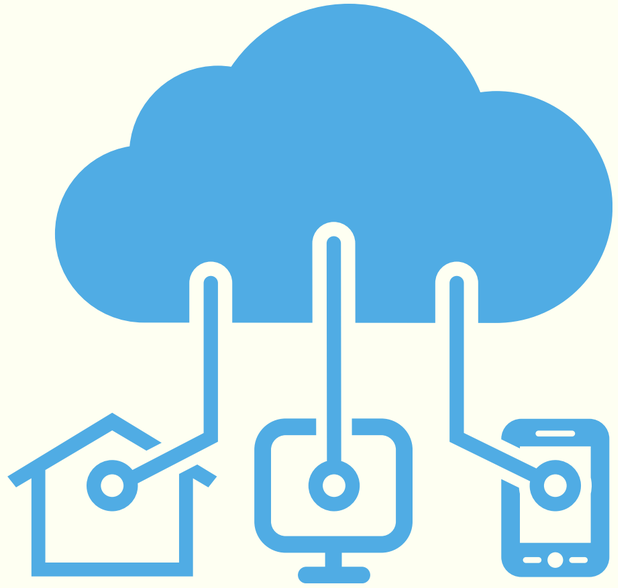
This calendar will feature a different topic each month to spread awareness of key aspects of cybersecurity and showcase ECSO members' and partners' solutions and services in the relevant areas to potential users.

The monthly themes for 2021 are planned as follows:

- January – Phishing
- February – Internet of Things
- March – Cloud Security
- April – Malware
- May – Ransomware
- June – Cybersecurity Skills
- July – Cyber Exercises
- August – Cybersecurity Summer School
- September – Mobile Devices & Bring Your Own Device (BYOD)
- October - Gender Diversity in Cyber
- November – Safer User Authentication & Password Hygiene
- December – Cybersecurity Trends 2022

DID YOU KNOW?

Facts & Figures about IoT



- The COVID-19 pandemic has accelerated IoT adoption globally - source
- According to IoT Analytics, in 2020, for the first time ever, the number of active IoT connections (e.g., connected cars, smart home devices, connected industrial equipment) surpassed the number of non-IoT connections (e.g., smartphones, laptops, and computers). By 2025, it is expected that there will be more than 30 billion IoT connections, or almost 4 IoT devices per person on the planet - source
- The enterprise IoT platform market will grow to $7.6 billion in 2024 with a 31% CAGR. Growth is driven by both on-premises and cloud deployments by the manufacturing, transportation and utility verticals, among other sectors. IoT PaaS is set to be the key enabler of IoT digital scenarios - source

MEMBER ECS
EUROPEAN CYBER SECURITY ORGANISATION

accenture

THE RAPID EXPANSION OF IOT HAS OPENED A PANDORA'S BOX FROM A SECURITY PERSPECTIVE

MORE INFO:

Security Blog
Cyber Threatscape Report
Security call to action: IoT (video)
Security call to action: IoT (slideshare)

The combination of powerful, low-cost smart connected devices and powerful cloud based big data analytics is giving unprecedented insights into the world in which we work, play and relax. However, the rich information streams and capabilities for sophisticated automation and remote access to goods and services are also extremely lucrative targets for cyber attackers.

The highly heterogeneous nature of the IOT means there is an overall lack of standards covering safety, privacy, security or reliability which, when combined with the change to remote working and purchasing habits driven by the COVID crisis, and a lack of security awareness amongst the general population, gives cybercriminals a wide and lucrative attack surface to exploit. Accenture has developed a **Smart Connected Products security capability** designed to embed security into every stage of an IOT product life cycle. It is backed by the Accenture Security practice with over 7500 exceptionally skilled security professionals worldwide who have extensive skills, covering Cyber Risk Assessment and remediation, Managed Security services, Secure IOT and Cloud Reference Architectures, Advanced Cyber Defense and penetration testing.

Internet of things

SECURITY RISKS IN THE INTERNET OF THINGS

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

By any chance, did you start a phrase today saying "Alexa", "OK, Google" or "Listen, Siri"? If so, you may have endangered your home or business. The Internet of Things (IoT) is growing exponentially, but many people are still unaware of the risks of smart devices. From Internet Segura programme belonging to Agència de Ciberseguretat de Catalunya (Cybersecurity Agency of Catalonia) we have worked on an article to help raise awareness of the dangers of having poorly configured IoT devices at home and 6 simple tips on how to avoid exposure. This trilingual INFOGRAPHIC on IoT - a joint project of the Internet Segura program of the Cybersecurity Agency of Catalonia and the ANTI-PHISHING WORKING GROUP EUROPEAN FOUNDATION.

By @internetambseny @apwg_eu #ECSO #CyberAwareness

CHECK OUT THE INFOGRAPHICS:

Infographic in English & Spanish

Infographic in Catalan

MEMBER ECS
EUROPEAN CYBER SECURITY ORGANISATION

ALIAS ROBOTICS
Robot Cybersecurity

CYBERSECURITY STANDS AS THE MAIN OBSTACLE FOR THE DEVELOPMENT OF INDUSTRIAL IOT

According to a recent study by the Massachusetts Institute of Technology “Industrial Internet of Things (IoT), perhaps the quintessential requisite for full cloud-based technology integration, has not yet been fully adopted by companies and remains in a pre-development stage. It is muddled by issues of privacy, questions over data ownership and autonomy, as well as security concerns” … “making sure that the entire robotic system, including the tasks that the human performs, is safe to work with should be a priority”. Traditional industrial cybersecurity solutions are obsolete in light of the massive incorporation of robots to operative environments. Robots require their own cybersecurity solutions.

Market intelligence suggests that 20% of industrial decision-makers (early adopters) are shifting to “zero-trust” cybersecurity approaches in their OT environments. Alias Robotics addresses this situation with the first robot endpoint cybersecurity solution. The Robot Immune System is now available for your own robots.

Learn more about Alias Robotics' solution here

Cyberwatch

Monitoring vulnerabilities on IoT devices require flexible methods

More info and a free demo of the product: Here

Monitoring vulnerabilities on IoT devices can be very hard based on network constraints: your devices can have a very low bandwidth, restricted network accesses, or irregular Internet connection.

A first approach consists in maintaining locally a copy of deployed devices, and assessing the vulnerabilities of your fleet based on your lab sample. Another approach is to fetch data from your fleet based on technical telemetry, and to assess the vulnerabilities of your deployed devices based on the actual data your received.

Cyberwatch provides a complete Vulnerability Management solution, deployed on premise, able to scan your vulnerabilities in both agent-based and agent-less modes. Moreover, Cyberwatch provides an air-gap assessment engine, to scan your assets based on direct data fetched from your telemetry with no direct connection between our scanners and your devices.

BUILDING CUTTING-EDGE IOT & OT CYBERSECURITY TO PROTECT DIGITAL TRANSFORMATION

Industry digitisation is about connecting industrial assets to get value from data and remote operations for enhanced efficiency, cost-reduction, and creation of new business models. Enigmedia aims to protect digitisation initiatives, securing data collection, communications on site and between remote sites, and IoT & OT network protection by developing advanced cybersecurity solutions. The company was founded in 2011, based on a patented system that allows encrypted communications with a negligible latency. This is critical for industrial and IoT communications. Just to give an example: in IT a latency below 100ms has no impact and is considered “real time” as the user cannot see any difference. However, in machine-to-machine communications, latency requirements are below 5/10ms! Indeed, with the advent of 5G we will see more strict time requirements.

More information can be found here.

Smart home privacy:
HOW TO AVOID ‘DATA PAPARAZZI’

With IoT devices becoming more prevalent, the users of these devices – and their behavior – are increasingly being observed and recorded. In this setting, it’s important to be aware of the data being collected and what it could reveal. Even the simplest data could reveal a lot of information, either on its own or when combined with other data sources. A poorly configured IoT deployment could turn out to be as intrusive as the paparazzi taking covert photographs of celebrities. Can we learn something from how celebrities deal with these privacy intrusion attempts? This blog looks at the data paparazzi problem and gives tips for how to improve your privacy.

Read the blog post here

MEMBER ECS
EUROPEAN CYBER SECURITY ORGANISATION

exprivia

Millions of interconnected IoT devices: HOW TO FACE SECURITY?

The Internet of Things is surrounding us with an ever-increasing number of IoT devices that can control industrial processes or common activities. Having those devices connected through the network make them vulnerable to external attacks. For this reason, it is strongly recommended to secure devices as they can be the entry point for compromising the service directly connected at the device. Protecting the IoT device is not helping just to be more secure, but helps to keep the entire ecosystem more secure. With regards to cybersecurity, with IoT it is clear that investment cannot be done just to secure the service, we need to invest to keep the entire ecosystem more secure. This is not a trivial difference in a world where investments are done based on ROI. In fact, it is not unusual to find, on the network, devices with default credentials or with missed security protocols which represent an easy attack surface (more information here).

An analyis by Exprivia's CyberSecurity Observatory in 2020 identified about 476M of interconnected devices on the planet. These devices include: cameras, routers, firewalls, smartTVs, printers, thermostats, medical devices and several other smart devices including PLC controlling industrial system (full analysis and graphs are available here).

Exprivia is committed to improving awareness on IoT security, researching vulnerabilities, participating in committees related to new protocols and helping customers to enable IoT devices in a secure way.

If you want to learn more about IoT, check out this course from Exprivia.

FIRMALYZER

DISCOVER IOT VULNERABILITIES IN A SAFE, AGENTLESS AND PRIVACY PRESERVING MANNER

Firmalyzer brings in-depth visibility of OT/IoT device vulnerabilities into your vulnerability management programme. It can be deployed as a standalone solution or integrated with your existing IT asset management and vulnerability assessment solution, providing continuous risk monitoring of IoT assets in enterprise networks without requiring network traffic collection or installation of software agents on IoT devices. Firmalyzer analysis dashboard will present security posture of all OT/IoT devices across different departments of your organisation that includes devices with critical and high risk vulnerabilities, devices with outdated firmware and discontinued devices that no longer receive firmware updates from the vendors. Firmalyzer not only detects publicly known vulnerabilities in IoT devices, but more importantly, it presents you with the deep firmware level vulnerabilities that are not found in public vulnerability databases such as CVE records that are widely used by traditional vulnerability scanning solutions.

More information can be found here.

MEMBER ECS
EUROPEAN CYBER SECURITY ORGANISATION

Fraunhofer AISEC

How safe is your IoT product?

SECURITY ASSESSMENT FOR CONNECTED IOT PRODUCTS

JOIN THE WORKSHOP:
In German
In English

Are you working on a product or service and would like to assess the security level? Do you want to know, if your current IT security concept meets the desired requirements or if you missed vulnerabilities? In this workshop, scientific security experts will review your (upcoming) IoT product.
The workshop addresses individual companies and allows to discuss a specific or upcoming IoT products, concepts or services with an individual selection of senior security analysts of Fraunhofer AISEC in all relevant sub-areas to get an external expert view. You receive immediate recommendations that you can implement.

EMBEDDED DEVICES AS A SECURITY HOLE

MEMBER ECS
EUROPEAN CYBER SECURITY ORGANISATION

Fraunhofer FKIE

Due to the increasing demands by their customers, many manufacturers try to make their devices smart by connecting them to the Internet. However, for many manufacturers this is a task where they have no previous knowledge and available experts are rare and expensive. In addition, modern software development often does not allocate time for well-thought-out security concepts. The situation becomes additionally challenging for small embedded devices due to the numerous communication standards available such as Wi-Fi, Zigbee or Bluetooth. In a hands-on workshop, our trainers explain these standards and show common security weaknesses and how-to avoid them. A head-start for every developer working on smart devices.

MORE INFO on the workshop:
Here

MEMBER ECS EUROPEAN CYBER SECURITY ORGANISATION

F-Secure

2021 predictions:

MASS IOT FAILINGS WILL SPARK ANOTHER MIRAI-LIKE ATTACK

Another worm or Mirai-like attack will occur in the next 1-3 years and reoccur periodically until effective quality control measures that address the security and privacy of internet-connected devices are widely implemented.

Read F-Secure's blog here.

THE INTERNET OF THINGS (IOT) AT HOME

You may have started a sentence with "Hey, Siri", "OK Google" or "Alexa" as the Internet of Things (IoT) is growing exponentially. It's a term we hear more and more often, but do you know what the IoT is all about? IoT devices can help us in many ways but we should not forget that they can also pose a threat. In this new post on Gaptain's "Education and Digital Wellbeing" blog we will look at the top 5 risks we can encounter when using IoT devices: Privacy issues, Security threats and malware, Theft, Device hijacking and Problems with voice commands. And if you want to be always informed and trained, we offer you our online programme for families "educating in digital" in video format so that you can consult it as, when and where you want.

More information can be found here.

GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

TRUSTCB®
TRUST AND VERIFY

SESIP methodology

DESIGNED AS THE ENABLER FOR THE IOT SECURITY ECOSYSTEM

The SESIP (Security Evaluation Standard for IoT Platforms) standard is an optimised methodology designed for IoT platforms, adopted by GlobalPlatform. SESIP offers a product centric approach to IoT Security, offering a framework where all the security actors have a common understanding of the security requirements and objectives. SESIP methodology supports a layered approach to security: by design, the reuse and the composition of products via the different components seen as layers, from bare metal hardware through IC dedicated firmware, security services such as Cryptography, Memory management and O/S to the application software, all of which combine to make the final product, are significantly simplified. SESIP defines 5 security levels directly mapped to the AVA_VAN assurance components "vulnerability analysis" from the Common Criteria. The SESIP assurance levels are complemented by relevant assurance components to provide the necessary level of information required for the security evaluation and certification of IoT devices. This includes, but is not limited to, secure update, secure life-cycle, secure communication, etc. GlobalPlatform provides mappings between SESIP and well-known security standards such as ETSI 303645, NISTIR8259, ARM PSA, IEC62443 and others. Additionally, thanks to multiple partnerships with the Industry, GlobalPlatform further aligns SESIP to be used in multiple IoT schemes. More information on SESIP is available here.

Internet of Things:

IOT SECURITY 3T + 1M FRAMEWORK

MEMBER ECS EUROPEAN CYBER SECURITY ORGANISATION

HUAWEI

True to its name, the Internet of Things (IoT) interconnects the things of our physical world and makes them available to applications. Owing to its potential direct impact on the physical world, security is of paramount importance in IoT. IoT security introduces technological challenges at the device, network and platform level. In addition, there is the process challenge of orchestrating the security technologies in an end-to-end manner. For these challenges, 3 key security technologies and 1 management capability are essential. In its efforts to ensure continued evolution and technological innovations in the 3T + 1M security architecture, Huawei considers a wide range a industry requirements for IoT cloud-pipe-device security, especially differentiated security requirements.

More information on Huawei's "3T+1M" IoT security architecture can be found here and here.

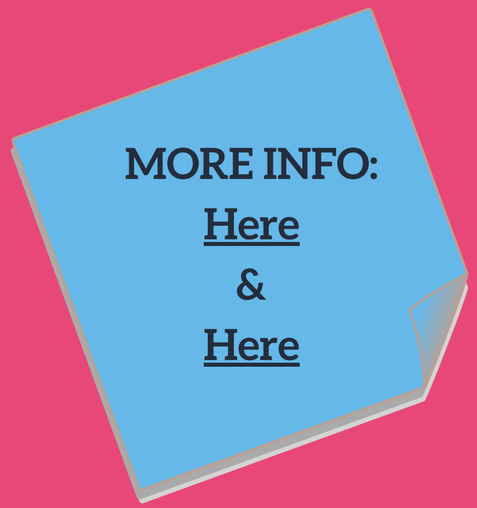
CYBERSECURITY CONSIDERATIONS IN THE ACQUISITION, INSTALLATION AND USE OF IOT DEVICES IN SMES

IoT devices are increasingly used by SMEs and become essential for their business. If using IoT devices we must consider some security procedures and tips to avoid security incidents. IoT devices are now a target for cyberattacks that may compromise, with serious consequences, our company security. At Spanish National Cybersecurity Institute (INCIBE) web page SMEs could find the IoT TemáTICa (in Spanish before 2/2/2021) and this Guide (Spanish), with information about:

- Risks in the use of IoT devices. IoT devices can be hacked and become part of botnets from which cybercriminals may launch other attacks such as denial of service, malware distribution, etc. In addition, IoT devices manage confidential information, which leakage could compromise companies' privacy.
- Know your enemy main attack vectors. Vulnerabilities, attacks based on social engineering, insecure communication channels, etc. Whatever cybercriminals use to compromise the security of IoT devices.
- Security measures to reduce the possibility of suffering a security incident and minimise the consequences in case it happens.

IoT Inspector

7,339 VULNERABILITIES WE RECEIVED FOR CHRISTMAS ARE STILL HAUNTING US IN FEBRUARY



IoT Inspector's security experts examined a fictitious gift basket containing six IoT devices from renowned manufacturers. They found a total of over 7,000 vulnerabilities.

The ever-increasing complexity of connected devices and the rising demand for security compliance in IoT calls for an efficient risk assessment approach. IoT Inspector's platform empowers manufacturers, service providers, enterprises, researchers, and users to run automated security analyses and identify compliance violations in their IoT devices before attackers exploit them. It is the easiest way to examine the device's firmware for vulnerabilities and its compliance with international security standards.

KEOPASS

Tired of dealing with complex passwords ?

USE KEOPASS BIOMETRIC KEY

KeoPass is the first standalone authentication device that generates complex passwords from fingerprints. The Biometric Key works with all smartphones and computers, via Bluetooth or USB, on any application or website that requires password authentication (including log-on), without any app/driver installation or API. The KeoPass Key can also replace existing RFID/NFC badges, adding biometric security to facilities and physical assets, without infrastructure modification.

Check it out here!

IS API SECURITY ON YOUR RADAR?

Gartner estimates that by 2021, exposed APIs will form a larger attack surface than UIs for 90 percent of web-enabled applications. APIs security challenges the classical paradigm of "professional team-based security", which entails that defense systems are maintained constantly by security personnel on a daily basis. Due to budget restraints and complexity issues, establishing and maintaining an effective API defense layer has become too expensive for most organisations, especially since relying on Web Application FW (WAFs) has shown to be inefficient for protecting applications and APIs against the latest cyberattacks. Therefore, a new type of security solution is needed to protect APIs.

More information can be found here.

MEMBER ECS
EUROPEAN CYBER SECURITY ORGANISATION

NASK

VULNERABILITY AND ATTACK REPOSITORY FOR IOT

Internet of Things devices are already ubiquitous and the related security problems are still insufficiently resolved. There are many risks associated with using IoT devices that users are unaware of. Therefore, care should be taken to raise the awareness of users. There are many threats related to the use of IoT devices - we use these devices in many applications and they affect our daily lives either directly or indirectly. We use smart washing machines, TV sets, smart toys, cameras; we can use them to control the operation of telemedicine devices, for diagnostics and therapeutic purposes. It can be very dangerous to use these devices intentionally or unintentionally against their intended purpose. This could be possible due to insufficient security or the emergence of new vulnerabilities. IoT devices are of course also used in military sectors and in critical infrastructure where security is a key issue. Therefore, NASK (https://en.nask.pl) is participating in the VARIoT project, as a result of which, by the end of this year, a repository of information about vulnerabilities and exploits in IoT devices will be created. The repository will be publicly available via European Data Portal. This project is co-financed by the Connecting Europe Facility of the European Union and the Polish Minister of Education and Science.

PARCOOR ON-DEVICE MALWARE DETECTION

Embedded systems and IoT objects are spreading at an increasingly fast pace as are attacks targeting them. At Parcoor we are developing a innovative malware detection solution. Our solution is based on a novel micro-event/deep-learning approach for protecting microcontrollers at their core. Concretely, in every microcontrollers or system on chip, we can find registers called hardware performance counters. These are registers of a processor able to count the occurrences of microarchitectural events that occur there, like branchmisses, LLC-load-misses etc. The idea here is to deploy deep learning algorithms on-device that will analyse those micro-events and correlate them with the execution of malware. There are several advantages to this but the 3 main ones are : low bandwidth and no middleware involved so the surface of attack does not increase, real-time detection and even zero day malware detection (no signature base to maintain), and last but not least, low energy consumption.

More information can be found here.

quadible

SECURING IOT DEVICES

People connect to and use services through a variety of devices i.e. PCs/Laptops, tablets, mobile phones or other means. And they typically still sign on for every service with their specific username-password combination. Data leaks and password thefts make regularly broadsheet headlines, and such cases underline the inadequacy of this authentication approach. The capabilities of IoT devices, and in particular those of smartphones have opened up the possibility to exploit user behaviour as additional features for the identification of an individual. Technologies like interaction behaviour, location patterns, etc. have proven to be efficient of identifying individuals using a certain observation period. Processing these individual observations together can be used to facilitate passive (for the user) authentication for accessing devices, services or content. Exploiting sensing data to derive behavioural cues and identify individuals. Quadible introduces the only solution offering Non Identifiable Unique Factor Behavioural Authentication, helping businesses mitigate fraud, improve the customer satisfaction while reducing costs. Quadible offers an AI-platform that continuously authenticates users and devices, without the need of any user input, by learning the behavioural patterns of the users and the IoT devices.

More information can be found here.

IoT Integration:

TOP 5 SECURITY QUESTIONS TO CONSIDER

MEMBER ECS
EUROPEAN CYBER SECURITY ORGANISATION

RED ALERT LABS
IoT Security

IoT has made it easier to be in the news headlines for the wrong reasons. As you think through IoT integration, it is important to gain clarity about the implication of installing those fancy IoT devices into your IT/OT infrastructure. Isaac Dangana a senior cybersecurity expert at Red Alert Labs proposes 5 important security questions to consider in this process. At Red Alert Labs, we offer IoT risk-based security approaches to help you qualify quickly and accurately the cyber-security risks covering your infrastructure, IoT product or solution and define the right set of security requirements, and countermeasures to be implemented. Speak to a security expert today and minimise the risk of hackers making you (in)famous.

More information can be found here.

MEMBER ECS EUROPEAN CYBER SECURITY ORGANISATION

secunet

IoT and intelligent Edge computing:

A PERFECT MATCH FOR MULTIFUNCTION AND SECURITY EFFICIENCY

Internet of Things (IoT) / Industrial Internet of Things (IIoT) is part of digitisation, for example for Industry 4.0. Understandably, the focus is primarily on the functional requirements for realising opportunities such as predictive maintenance, remote service or data transfer for optimised planning. Intelligent decentralisation in the form of edge computing is gaining ground, as data processing is useful directly on site and directly at the system - e.g. through real-time capability, protocol translations, data minimisation and consolidation. At the same time, new and attractive cyber-attack surfaces are emerging through malware and errors. The entire digital functionality and connectivity must therefore be comprehensively protected and should ideally already be part of the edge infrastructure. Secunet edge addresses these and other challenges of edge computing as an industrial, multifunctional, secure and trustworthy edge platform.

More information can be found here.

IOT: IT A BLESSING OR A CURSE?

MEMBER ECS EUROPEAN CYBER SECURITY ORGANISATION

SECURITY MADEIN.LU

circl.lu cases.lu c-3.lu

READ THE ARTICLE:
Here

Connected objects have gradually invaded our daily life. The Internet of Things (IoT) brings together all the sensors and objects connected to the Internet, thus allowing remote control of our physical environment. Among the new technological trends, IoT increasingly plays a predominant role.

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

SAMSUNG INNOVATION CAMPUS - SMART THINGS EDITION

Samsung Innovation Campus - Smart Things Edition is an educational path developed by Samsung in partnership with some of the best Italian public universities aimed at providing students of technical-scientific paths with the AI, IoT, and soft skills necessary to drive the digital transformation that is revolutionising the production and organisational dynamics of companies.

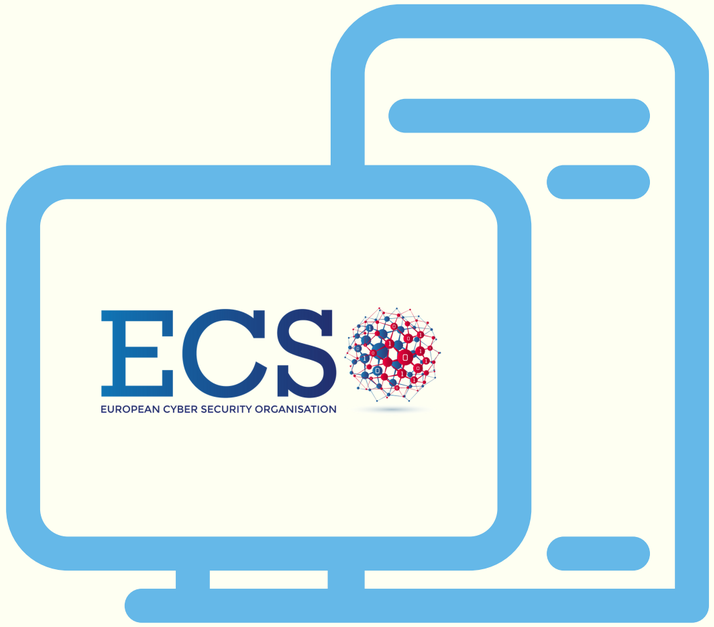
The course trains on the application of IoT and AI technologies in the Consumer Electronics product market, transfers skills of ideation, project management and problem solving and prepares for professional placement. The course includes 100 hours of digital learning, 65 hours of in-class lectures held by Samsung and University professors and 80 hours of teamwork in which students develop their own project. In February 2021, the course will be active at the Department of Computer Science of the University of Bari "Aldo Moro".

Check it out HERE!

THANK YOU!

for your time

Cybersecurity Awareness Calendar is an initiative launched by:
European Cyber Security Organisation (ECSO)
29, rue Ducale
1000 - Brussels



www.ecs-org.eu

secretariat@ecs-org.eu

/company/ecso-cyber-security/

@ecso_eu